

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates - Huawei

Tracking #:432317568

Date:05-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Huawei has released security updates to address multiple vulnerabilities in its flagship models.

TECHNICAL DETAILS:

HUAWEI has released its August 2025 security bulletin for HarmonyOS and EMUI devices, addressing multiple high- and medium-severity vulnerabilities across various system components and third-party libraries. These vulnerabilities, if exploited, may impact confidentiality, availability, stability, or service integrity of affected devices.

Vulnerability Details (including but not limited to):

CVE	Description	Impact	Severity
CVE-2025-54607	Authentication management vulnerability in the ArkWeb module	Successful exploitation of this vulnerability may affect service confidentiality.	High
CVE-2025-54611	EXTRA_REFERRER resource read vulnerability in the Gallery module	Successful exploitation of this vulnerability may affect service confidentiality.	High
CVE-2025-54622	Binding authentication bypass vulnerability in the devicemanager module	Successful exploitation of this vulnerability may affect service confidentiality.	High
CVE-2025-54627	Out-of-bounds write vulnerability in the skia module	Successful exploitation of this vulnerability may affect service confidentiality.	High

Affected/Fixed Versions: Refer [Security Bulletins for HUAWEI Phones/Tablets, August 2025](#)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying latest updates released by the Huawei.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://consumer.huawei.com/en/support/bulletin/2025/8/>